

sending at least one verification response, based upon the comparing of the first fingerprint file against the second fingerprint file and upon the comparing of the first identification for the user against the second identification for the user.

6. The method according to claim 5 wherein the verification computer is a clearinghouse computer.

7. The method according to claim 5 wherein the verification computer is a vendor computer.

8. A method according to claim 5, wherein said step of sending at least one request to a user computer includes:

    sending a first request to the user computer for the first fingerprint file; and

    sending a second request to the user computer for the first identification for the user.

9. A method according to claim 5, wherein said step of receiving at least one response from the user computer includes:

    receiving a first response from the user computer including the fingerprint file; and

    receiving a second response from the user computer including the first identification for the user.

10. A method according to claim 9, wherein the second response from the user computer is received prior to first response from the user computer.

11. A method according to claim 5, wherein said steps of comparing the first fingerprint file against a second fingerprint file, and comparing the first identification for the user against a second identification for the user are not performed simultaneously.

12. A method according to claim 7, wherein said step of sending at least one response to the vendor computer, based upon the comparing of the first fingerprint file against the second

fingerprint file and upon the comparing of the first identification for the user against the second identification for the user includes sending a confirmation only when both the first fingerprint file and the first identification of the user match the second fingerprint file and the second identification for the user respectively.

13. A method according to claim 8, wherein said step of receiving at least one response from the user computer includes:

receiving a first response from the user computer including the first fingerprint file; and  
receiving a second response from the user computer including the first identification for

the user.

14. A method according to 13, wherein the second response from the user computer is received prior to first response from the user computer.

15. A method according to claim 5, wherein the first identification for the user includes a password.

16. A method according to claim 5, wherein the first fingerprint file includes information based upon an identification number of a CPU of the user computer.

17. A method according to claim 5, wherein the first fingerprint file includes information based upon a MAC address associated with the user computer.

18. A method according to claim 5, wherein prior to the step of receiving the first request from the verification computer,

storing the second fingerprint file in a first data base accessible by verification computer,

and

storing the second identifications for the user in a second database accessible by the verification computer.

19. A method according to claim 7, wherein prior to the step of receiving the first request from the vendor computer,

storing the second fingerprint file in a first data base accessible by a clearinghouse computer, and

storing the second identifications for the user in a second database accessible by a clearinghouse computer.

20. A method according to claim 17, wherein the first database and second database are the same.

21. A method according to claim 7, wherein the step of receiving a request from a vendor computer includes receiving an internet address of the user computer.

22. A method according to claim 21, wherein prior to the step of sending the at least one request to the user computer, identifying the user computer based upon the internet address received from the vendor computer.

23. A clearinghouse computer comprising:

a storage unit for storing information received from a user computer; the information including a second fingerprint file and a second identification for a user;

a memory unit for receiving information indicative of first fingerprint file and a first identification for the user; and

a processor for communicating with the storage unit and the memory unit for comparing information indicative of the second fingerprint file and the second identification for the user with information indicative of the first fingerprint file and first identification for the user, and causing a message to be generated based upon the comparing.

24. A clearinghouse computer according to claim 23, wherein the storage unit includes:

a first storage location for storing the second fingerprint file, and

a second storage location for storing the second identification for the user.

25. A clearinghouse computer according to claim 23, wherein the memory unit includes:

a first memory location for storing, at least temporarily, the first fingerprint file, and

a second memory location for storing, at least temporarily, the first identification for the

user.

26. A clearinghouse computer according to claim 23, further including:

an output for receiving the message to be generated based upon the comparison, and

the output further capable of communicating with a vendor computer.

27. A clearinghouse computer according to claim 23, wherein the second identification for the user includes a password.

28. A clearinghouse computer according to claim 23, wherein the second fingerprint file includes information based upon an identification number of a CPU of the user computer.

29. A method for verifying a user and a user computer comprising:

receiving at a first server at least one first message from the user computer, the at least one first message including a first fingerprint file;

comparing the first fingerprint file against a second fingerprint file to verify the user computer, the second fingerprint file accessible by the first server;

receiving at a second server at least one second message from the user computer, the at least one second message including a first identification for the user; and

comparing the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the second server.

30. A method according to claim 29 where at least one server is a mini-server

31. The method according to claim 30 where the first and second servers are mini-servers.

32. A method according to claim 31, wherein the first mini-server is associated with a first clearinghouse computer and the second mini-server is associated with a second clearinghouse computer.

33. A method according to claim 31, wherein the first mini-server is associated with a first clearinghouse computer and the second mini-server is associated also with the clearinghouse computer.

34. A method according to claim 29, wherein:

after the step of comparing the first fingerprint file against the second fingerprint file to verify the user computer, generating a first-mini-server message at the first mini-server based upon the results of said comparison; and

after the step of comparing the first identification for the user against the second identification for the user to verify the user, generating a second-mini-server message at the second mini-server based upon the results of said comparison.

35. A method according to claim 34, further including:

sending the first-mini-server message to a vendor computer; and

sending the second-mini-server message to the vendor computer.

36. A method according to claim 35, further including:

authorizing an action by the vendor computer only if both the first-mini-server message contains information indicating the user computer was verified and the second-mini-server message contains information indicating the user was verified.

37. A vendor computer comprising:

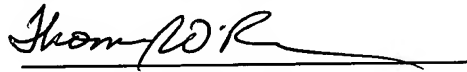
a first input for communicating with a first mini-server for receiving a first-mini-server message containing information indicating if a user computer was verified;

a second input for communicating with a second mini-server for receiving a second-mini-server message containing information indicating if a user was verified;

a processor for receiving the first-mini-server message from the first output and the second mini-server message from the second output and authorizing an action only if both the first-mini-server message contains information indicating the user computer was verified and the second-mini-server message contains information indicating the user was verified.

38. A vendor computer according to claim 37, wherein the first input and the second input are the same.

Respectfully submitted,



Thomas A. O'Rourke

Reg. No.: 27,665

BODNER & O'ROURKE, L.L.P.

425 Broadhollow Road

Melville, New York 11747

(631) 249-7500